



(11) **EP 2 409 479 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
12.07.2017 Bulletin 2017/28

(51) Int Cl.:
H04M 1/725 (2006.01) H04L 29/08 (2006.01)

(21) Application number: **10708615.9**

(86) International application number:
PCT/IB2010/050820

(22) Date of filing: **25.02.2010**

(87) International publication number:
WO 2010/106452 (23.09.2010 Gazette 2010/38)

(54) **METHOD FOR TOP-UP INFORMATION AND COMPUTER DEVICE**

VERFAHREN FÜR ZUSATZINFORMATIONEN UND RECHNERGERÄT

PROCÉDÉ POUR INFORMATIONS D'APPOINT ET DISPOSITIF INFORMATIQUE

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL
PT RO SE SI SK SM TR**

(30) Priority: **19.03.2009 EP 09290206**

(43) Date of publication of application:
25.01.2012 Bulletin 2012/04

(73) Proprietor: **NXP B.V.
5656 AG Eindhoven (NL)**

(72) Inventors:
• **CORDA, Alexandre**
Redhill Surrey RH1 1DL (GB)
• **LEMONNIER, Vincent**
Redhill Surrey RH1 1DL (GB)
• **AFFOUARD, Baptiste**
Redhill Surrey RH1 1DL (GB)

(74) Representative: **Krott, Michel**
NXP B.V.
Intellectual Property & Licensing
High Tech Campus 60
5656 AG Eindhoven (NL)

(56) References cited:
• **GSMA: "mobile NFC technical guidelines -
Version 2.0" INTERNET CITATION November
2007 (2007-11), pages 1-95, XP002495767**
Retrieved from the Internet:
URL: http://www.gsmworld.com/documents/nfc/gsma_nfc2_wp.pdf [retrieved on 2008-09-09]
• **NORDLUND S: "Secure Over-The-Air Services in
NFC Ecosystems" INTERNET CITATION 20 March
2007 (2007-03-20), XP002470503 Retrieved from
the Internet:**
URL: http://www.nfc-research.at/fileadmin/congress/pdf/05_Venyon_Sirpa_Nordlund.pdf [retrieved on 2008-02-25]
• **GSMA: "Mobile NFC Services" INTERNET
CITATION 1 February 2007 (2007-02-01), pages
1-24, XP002510722 Retrieved from the Internet:**
URL: http://www.gsmworld.com/documents/nfc_services_0207.pdf [retrieved on 2009-01-16]

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 409 479 B1

Description

FIELD OF THE INVENTION

[0001] The invention relates to a method for top-up information and to a computer device.

BACKGROUND OF THE INVENTION

[0002] Near Field Communication, abbreviated "NFC", is a short-range high frequency wireless communication technology enabling exchange of data between devices within a relative short distance, for instance, about 10 centimeters. NFC is based on RFID (radio frequency identification) and combines an interface of a smartcard and a reader into a single device. NFC devices can communicate with RFID readers and with other NFC devices and may, for instance, be mobile phones.

[0003] Business opportunities presented by using NFC enabled mobile devices, such as mobile phones, for, for instance, contactless payment, transport ticketing, loyalty and other services may be of interest, for instance, for mobile operators and service providers in the banking, transport and retail sectors.

[0004] For addressing operational requirements, NFC utilizes a so called Trusted Service Manger (TSM) which is supposed to help service providers to securely distribute and manage, for instance, contactless services for their customers utilizing networks of mobile operators. Fig. 1 illustrates how a Trusted Service Manager Backend 1 is conventionally used to transmit an NFC application 9 issued by a Service Provider Backend 2 (service provider web site) to a mobile telephone 3 comprising NFC capability.

[0005] If the service provider wants to issue the NFC application 9 to the mobile phone 3, he connects his Service Provider Backend 2 to the mobile phone 3 through the Trusted Service Manager Backend 1. The Trusted Service Manager Backend 1 establishes a secure channel to transmit the NFC application 9 over the air OTA to the mobile phone 3 which includes an appropriate interface which is, for instance, a GSM interface not explicitly shown in the figures.

[0006] The mobile phone 3 comprises a proxy 4, a secure application 5, also known as "wallet" or trusted application, to present information about NFC applications already installed on the mobile phone 3 to the user of the mobile phone 3, an NFC module including a Service Manager 6 and a memory 7 to store the NFC application. The secure application 5 is also responsible to allow the user to top-up applications, for instance, to request to reload an NFC application. If, for instance, the NFC application is associated with an e-purse, the request may, for instance, be a request to reload money on this e-purse.

[0007] Top-up information is located in the secure application 5 (wallet) itself. Top-up information is proprietary formatted information. Therefore, if a new NFC application is issued to the mobile phone 3 by a new service

provider, the user has to install an up-dated version of his/her wallet including top-up information for this new NFC application.

[0008] It is an object of the invention to provide an improved method to top-up information particularly usable by wallets. Further related art is "GSMA: "mobile NFC technical guidelines - Version 2.0", INTERNET CITATION, November 2007 (2007-11), pages 1-95, XP002495767".

OBJECT AND SUMMARY OF THE INVENTION

[0009] The object of the invention is achieved by means of a method for processing top-up data according to claim 1. The object of the invention is also achieved by means of a computer device, comprising a server device configured to carry out the inventive method. If an NFC mobile device, such as a mobile hand set, for instance, a mobile phone, needs top-up an application, particularly an NFC application run on the mobile device, the mobile device needs to contact the appropriate Service Provider to have him issue the requested application. Since it may happen that the request sent by the mobile device does not comply with the Service Provider's needed information, the communication between the NFC mobile device and the Service Provider Backend cannot be directly performed. Due to the transforming of the data sent by the mobile phone into data formatted such they comply with the addressed Service Provider, the Service Provider, i.e. its Backend can transfer the requested top-up or NFC application to the mobile device utilizing, for instance, the well known Trusted Service Manager.

[0010] The server transforming the data may be associated with the Trusted Service Manager or may be part of the Trusted Service Manager. Since the Trusted Service Manager manages loading up requested NFC applications or their top-ups, the Trusted Service Manager can centrally administer the transforming of the reformatting data in a relatively effective manner.

[0011] Transforming the data into a format complying with the Service Provider may be carried out by reformatting the data into a format complying with the Service Provider.

[0012] The data related to the request may include information retrieved from a secure application of the mobile device. A secure application is also referred to as "wallet". Normally, in an NFC ecosystem, it is the responsibility of this wallet, which is also called "trusted application", to present to the user of the mobile device information about the NFC applications already installed in the NFC mobile device. Usually, the purpose of the wallet is also to allow the user to top-up, i.e. to request to reload an NFC application. An example of such a request is to request to reload a certain amount of money, for instance, 15 Euros on his/her NFC e-purse, if the mobile device comprises such an e-purse.

[0013] The retrieved information may particularly be related to the user of the mobile phone particularly to an

ID of the user. Then, the Service Provider can allocate the request to the appropriate mobile device and to the appropriate user. The latter may be important if the Service Provider needs to contact the user or bill him/her for the request.

[0014] In order to transform the ID retrieved by the secure application and received at the server, the server may be configured to transform the format of the ID as retrieved by the secure application to a format complying with the Service Provider. As discussed above, it may happen that the Service Provider does not understand the request sent by the mobile phone directly, for instance, if the user ID required by Service Provider Backend may be different from the user ID added by the secure application (wallet). Due to the inventive computer device, i.e. the introduced server, a particularly common formatted data related to the request sent by the mobile device is translated into proprietary data, particularly top-up data, understandable by the Service Provider, i.e. its Backend.

[0015] Applications of the inventive method or the inventive computing device may comprise NFC mobile devices, such as NFC mobile phones, over the air (OTA) provisioning, NFC applications and top-up reloading.

[0016] These and other aspects of the invention are apparent from and will be elucidated with reference to the embodiments described hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The invention will be described in greater detail hereinafter, by way of non-limiting examples, with reference to the embodiments shown in the drawings.

Fig. 1 is a diagram illustrating transferring an NFC application from a Trusted service provider to an NFC device in a conventional manner;

Fig. 2 is a diagram illustrating a method to top-up an NFC application; and

Fig. 3 is a flow chart illustrating the top up of the NFC application.

DETAILED DESCRIPTION OF EMBODIMENTS

[0018] Fig. 1 has been discussed in the introduction.

[0019] Fig. 2 shows the mobile phone 3 as an example of a hand set which includes NFC capabilities. The mobile phone 3 is thus an example of an NFC mobile device.

[0020] Fig. 2 further shows the Trusted Service Manager Backend 1 and the Service Provider Backend 2 operated by the Service Provider.

[0021] Each time a new NFC application is issued to the mobile phone 3, the secure application 5 ("wallet") retrieves specific information about this NFC application, step A of the flow chart of Fig. 3. This task may be, for instance, performed when the relevant NFC application is issued, once a day, or on the user's demand. The secure application 5 also retrieves top-up data correspond-

ing to the relevant application. The top-up data correspond to the specific NFC application and usually do not comprise information about the user at this step.

[0022] When the user of the mobile phone 3 requests a top-up, the secure application 5 processes the top-up data to add information related to the current user, for instance, the user's ID, step B of the flow chart of Fig. 3.

[0023] For instance, if the mobile phone 3 requests the top-up data from a new service provider, then the top-up data sent from the mobile phone 3 generally do not match the information or format needed for processing the request by the relevant Service Provider Backend 2. For instance, the format of the user's ID required by the current Service Provider Backend 2 may differ from the format of the user's ID added by the secure application 5. Then, direct communication between the mobile phone 3 and the Service Provider Backend 2 for issuing the NFC application 9 is not possible.

[0024] For the exemplary embodiment, a server, from now on denoted as top-up server 8, is utilized. The top-up server 8 may be linked to the Trusted Service Management Backend 1 or may even be incorporated into the Trusted Service Management Backend 1.

[0025] For the exemplary embodiment, if the mobile phone 3 requests the new NFC application 9, the mobile phone 3, utilizing its secure application 5, does not connect directly to the relevant Service Provider Backend 2 utilizing, for instance, the service provider's URL (Uniform Resource Locator), but sends the request including the top-up data and the service provider's URL to the top-up server 8, step C of the flow chart of Fig. 3. The top-up server 8 is configured to accept and to process the request in order to transform the request into a format acceptable to the addressed Service Provider Backend 2. For this purpose, the top-up server 8 may include a table or a data base which includes information about the specific formats required by several Service Provider Backends 2 utilizing, for instance, their URLs.

[0026] As a result, the top-up server 8 is configured to translate a common format for top-up data, i.e. NFC application related data as well as information added by the secure application 5, into proprietary top-up data which the relevant Service Provider Backend 2 can understand and thus process.

[0027] Then, the top-up server 8 connects to the addressed Service Provider Backend 2 utilizing, for instance, its URL and transfers the reformatted request which complies with the format of the relevant Service Provider, step D of the flow chart.

[0028] The addressed Service Provider Backend 2 can then check the validity of the transformed top-up data and can perform certain specific actions associated with the request, such a sending a bill to the user, step E of the flow chart.

[0029] For the exemplary embodiment, the Service Provider Backend 2 connects then to the Trusted Service Management Backend 1 to request to load the requested NFC application 9 to the mobile phone 3, step F of the

flow chart. Then, the Trusted Service Manager Backend 1 transfers the NFC application 9 to the mobile phone 3, step G of the flow chart.

[0030] Finally, it should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be construed as limiting the claims. The word "comprising" and "comprises", and the like, does not exclude the presence of elements or steps other than those listed in any claim or the specification as a whole. The singular reference of an element does not exclude the plural reference of such elements and vice-versa. In a device claim enumerating several means, several of these means may be embodied by one and the same item of software or hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

Claims

1. A method for processing top-up data, comprising the steps of:

- receiving at a server (8) a request for issuing an NFC application (9) which is sent by an NFC mobile device (3) and is intended for a Service Provider (2), wherein said request includes top-up data having a common format;
- generating at the server (8) a reformatted request by transforming the top-up data into a proprietary format complying with the Service Provider (2), and
- transferring the reformatted request to the Service Provider (2) for further processing and for issuing the NFC application (9) to the mobile device (3).

2. The method of claim 1, wherein the top-up data include information retrieved from a trusted application (5) of the mobile device (3) and/or the URL of the Service Provider (2).

3. The method of claim 2, wherein the information is related to the user of the mobile phone (3) particularly an ID of the user.

4. The method of claim 3, comprising transforming at the server (8) the format of the ID as retrieved by the trusted application (5) to a format complying with the Service Provider (2).

5. The method of claim 1, wherein the server (8) is associated with the Trusted Service Manager (1) or the

Trusted Service Manager (1) comprises the server (8).

6. The method of claim 1, wherein the NFC mobile device is a mobile hand set, particularly a mobile phone (3).
7. A computer device, comprising a server device (8) configured to carry out the method of any of claims 1 to 6.
8. The computer device of claim 7 being associated with a Trusted Service Manager (1) or being part of the Trusted Service Manager (1).

Patentansprüche

1. Ein Verfahren zum Verarbeiten von Top-Up Daten, aufweisend die Schritte:

Empfangen an einem Server (8) einer Anfrage zum Ausgeben einer NFC Anwendung (9), die durch eine NFC mobile Vorrichtung (3) gesendet wird und intendiert ist für einen Service Provider (2), wobei die Anfrage Top-Up Daten enthält, die ein geläufiges Format haben;
Erzeugen an dem Server (8) einer re-formatierten Anfrage mittels Transformierens der Top-Up Daten in ein proprietäres Format, das mit dem Service Provider (2) in Einklang steht, und
Transferieren der re-formatierten Anfrage an den Service Provider (2) zum weiteren Bearbeiten und zum Ausgeben der NFC Anwendung (9) an die mobile Vorrichtung (3).

2. Das Verfahren gemäß Anspruch 1, wobei die Top-Up Daten eine Information umfasst, die erhalten wurde von einer vertrauenswürdigen Anwendung (5) von der mobilen Vorrichtung (3) und/oder der URL von dem Service Provider (2).

3. Das Verfahren gemäß Anspruch 2, wobei die Information in Beziehung steht zu dem Nutzer von dem Mobiltelefon (3), insbesondere einer ID von dem Nutzer.

4. Das Verfahren gemäß Anspruch 3, aufweisend Transformieren an dem Server (8) des Formates von der ID, wie erhalten durch die vertrauenswürdige Anwendungen (5), in ein Format, das in Einklang steht mit dem Service Provider (2).

5. Das Verfahren gemäß Anspruch 1, wobei der Server (8) assoziiert ist mit dem Trusted Service Manager (1) oder der Trusted Service Manager (1) den Server (8) aufweist.

- | | |
|--|---|
| <p>6. Das Verfahren gemäß Anspruch 1, wobei die NFC mobile Vorrichtung ein mobiles Hand-Set ist, insbesondere ein Mobiltelefon (3).</p> <p>7. Eine Computervorrichtung aufweisend eine Servervorrichtung (8), die konfiguriert ist zum Ausführen des Verfahrens gemäß einem der Ansprüche 1 bis 6.</p> <p>8. Die Computervorrichtung gemäß Anspruch 7, wobei diese assoziiert ist mit einem Trusted Service Manager (1) oder die Teil ist von dem Trusted Service Manager (1).</p> | <p>7. Dispositif informatique comprenant un dispositif serveur (8) configuré pour exécuter le procédé selon l'une quelconque des revendications 1 à 6.</p> <p>8. Dispositif informatique selon la revendication 7 étant associé à un gestionnaire de services de confiance (1), ou faisant partie du gestionnaire de services de confiance (1).</p> |
|--|---|

Revendications

- | | |
|--|---|
| <p>1. Procédé de traitement de données d'appoint, comprenant les étapes suivantes :</p> <p style="padding-left: 40px;">- recevoir, au niveau d'un serveur (8), une demande d'émission d'une application NFC (9) qui est envoyée par un dispositif mobile NFC (3) et qui est destinée à un fournisseur de services (2), où ladite demande comprend des données d'appoint ayant un format commun ;</p> <p style="padding-left: 40px;">- générer, au niveau du serveur (8), une requête reformatée en transformant les données d'appoint en un format propriétaire conforme au fournisseur de services (2), et</p> <p style="padding-left: 40px;">- transférer la demande reformatée au fournisseur de services (2) pour un traitement ultérieur et pour délivrer l'application NFC (9) au dispositif mobile (3).</p> <p>2. Procédé selon la revendication 1, dans lequel les données d'appoint comprennent des informations extraites d'une application de confiance (5) du dispositif mobile (3) et/ou l'URL du fournisseur de services (2).</p> <p>3. Procédé selon la revendication 2, dans lequel les informations concernent l'utilisateur du téléphone mobile (3), en particulier un identifiant de l'utilisateur.</p> <p>4. Procédé selon la revendication 3, comprenant de transformer, au niveau du serveur (8), le format de l'ID tel que récupéré par l'application de confiance (5) en un format se conformant au fournisseur de services (2).</p> <p>5. Procédé selon la revendication 1, dans lequel le serveur (8) est associé au gestionnaire de services de confiance (1), ou le gestionnaire de services de confiance (1) comprend le serveur (8).</p> <p>6. Procédé selon la revendication 1, dans lequel le dispositif mobile NFC est un combiné sans fil, en particulier un téléphone mobile (3).</p> | <p>15</p> <p>20</p> <p>25</p> <p>30</p> <p>35</p> <p>40</p> <p>45</p> <p>50</p> <p>55</p> |
|--|---|

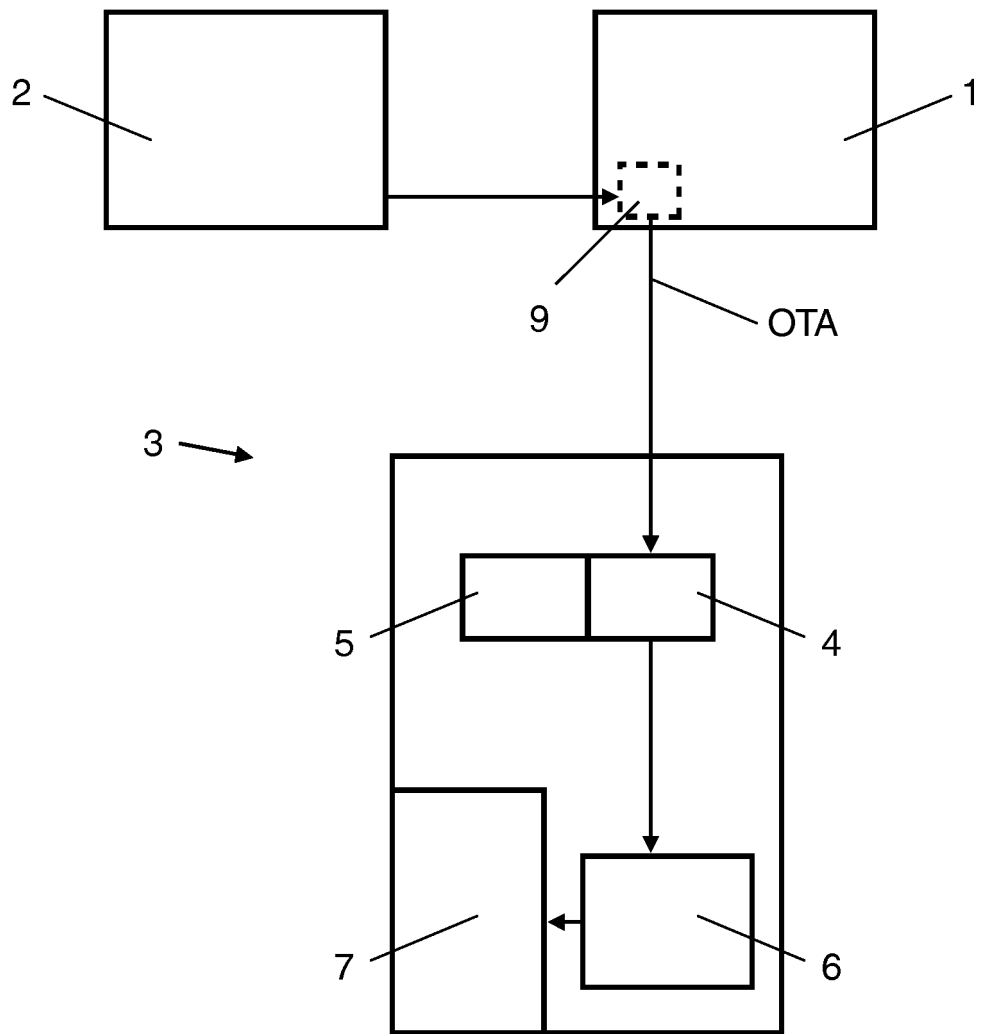


FIG. 1

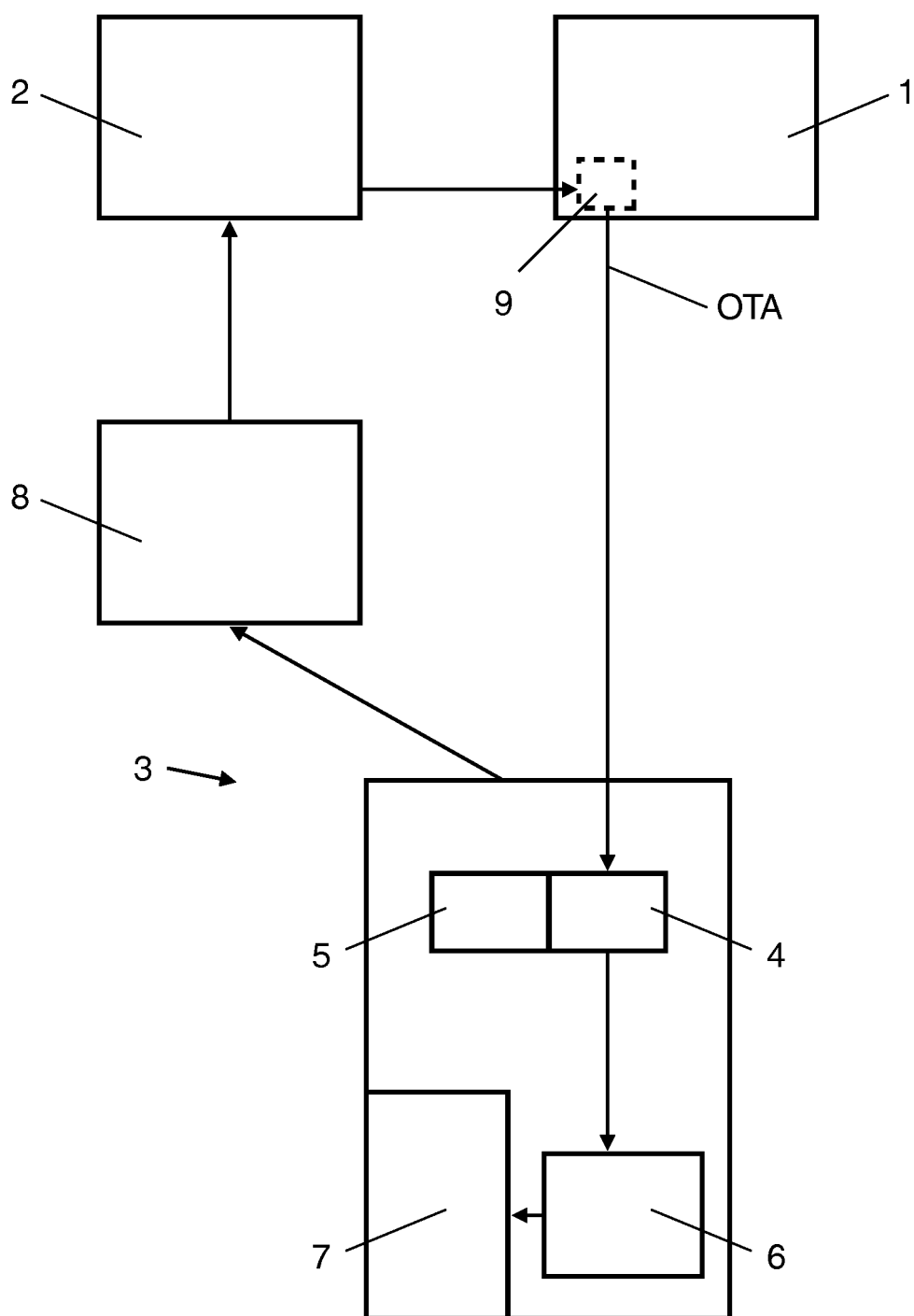


FIG. 2

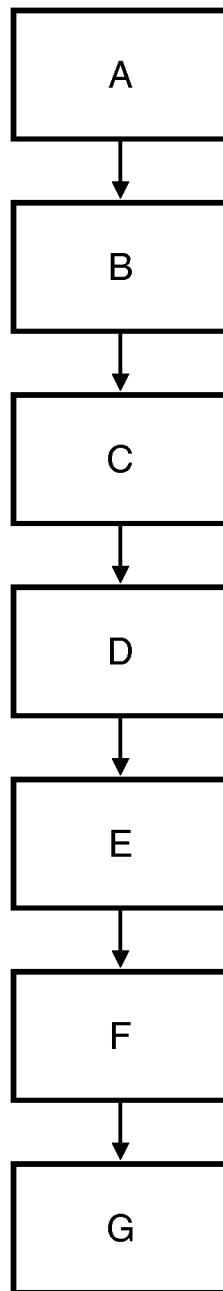


FIG. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- GSMA: "mobile NFC technical guidelines - Version 2.0. *INTERNET CITATION*, November 2007, 1-95
[0008]